

Security and Disaster Recovery Electronic Message Privacy Policy

in Washington State Government

September 1991

Prepared by:
Washington State
Department of Information Services
George Lindamood, Director
PO Box 42440
Olympia, WA 98504-2440

Adopted by:
Washington State
Information Services Board
Len McComb, Chair

Introduction

The effective management and application of information technology improves the quality of service delivered to Washington's citizens, the productivity of the state workforce, and the overall cost effectiveness of state operations. Electronic message systems (electronic mail, voice messaging, and image transmission) play an increasingly important role in meeting this challenge.

Agencies may wish to implement agency policies for electronic message system privacy. This guideline provides a sample policy that is aimed at managing expectations: Just what level of electronic message privacy should employees expect in a state government environment?

The sample agency policy that follows defines the permissible use of agency electronic message systems and the grounds on which agencies will access messages without the sender or receiver's consent. This policy tells employees that the agency has the right to monitor all electronic information.

Sample Agency Policy

This policy applies to all agency employees using agency message systems to conduct agency business.

The effective management and application of information technology improves the quality of service delivered to Washington's citizens, the productivity of the state workforce, and the overall cost effectiveness of state operations. Electronic mail, voice messaging, and image transmission systems play an increasingly important role in meeting this challenge.

Employees should use agency electronic message systems only to conduct agency business.

All agency information technology resources, including electronic messaging systems, are the property of the state of Washington.

Agency electronic message systems shall not be used for transmission of information that promotes:

- Discrimination on the basis of race, creed, color, gender, religion, handicap, or sexual preference;
- Sexual harassment;
- Copyright infringement;

- Personal political beliefs;
- Personal business interests; or
- Any unlawful activity.

Electronic message systems are not secure.

Because electronic messages are typically stored in one place and then forwarded to multiple locations, they are vulnerable to interception. Users of electronic messaging systems should be aware of the basic types of electronic messaging security violations:

- Disclosure: an unauthorized user gaining access to the information contained in electronic messages. Disclosure often occurs inadvertently when messages are forwarded to unauthorized users or are printed in a common use area where others can read them. Pass code disclosure, whether between authorized users or by a hacker, can also lead to violations.
- Message modification: altering a message to modify its contents or delivery time. This might be done by an authorized or unauthorized user.
- Masquerading: an authorized user who appears to the system to be another user, usually one with higher privileges, to gain access to information or resources.
- Repudiation: an authorized user who denies having sent a message or denies having received a message. This violation becomes very important in electronic data interchange applications where business transactions such as purchase orders and invoices are performed as electronic messages.

The agency will attempt to provide electronic messaging systems that provide data confidentiality and integrity.

Public records contained on electronic message systems should be maintained according to retention schedules approved by the appropriate records committee in accordance with the Revised Code of Washington (RCW) Chapter 40-14.

While all electronic messages may be considered writings, and all writings may be public records, the public does not have a right to examine every public record. RCW Chapter 42.17 exempts broad categories of records, while other statutes provide for confidentiality of specific records.

The agency reserves the right to monitor all electronic messages.

The agency will not monitor electronic message transmissions on a regular basis. The construction, maintenance, repair, and operation of electronic message

systems may occasionally result in monitoring random transmitted or stored electronic messages.

Messages may be monitored to prevent misuse of the system. They may also be monitored or during the course of investigations of illegal activity.

Agency managers have access to data (including electronic messages) under their individual employee's control when necessary to conduct agency business.

The agency will not provide third parties with access to stored electronic messages without the consent of the sender or recipient except in special circumstances, such as; to resolve a technical problem with a system or investigations of illegal activity or misuse of the system.

Electronic messages are often stored in order to backup the applications processing performed by electronic messaging systems. Agency employees should assume that all electronic messages are stored for a period of (nn) days on (specific media).

Requests for third-party access to stored electronic messages without the consent of the sender or recipient must be approved by the agency director.

Definitions

The following definitions apply to this guideline:

- **"Security"** means something that assures safety; protection or defense.
- **"Privacy"** means secrecy.
- **"Electronic message systems"** include electronic mail (E-mail) systems which store and transmit typed communications, voice mail systems which store and transmit voice communications, facsimile and imaging equipment which store and transmit images, and all similar systems.
- **A "public record"**, as defined by RCW 42.17.020(26), includes "any writing which contains information relating to the conduct of government or the performance of any governmental or proprietary function."
- **A "writing"**, as defined by RCW 42.17.020(28), includes all means of recording any form of communication or representation, including documents, pictures, computer tapes or disks, and sound recordings.